



Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions



Systems
Engineering
Solutions

ManTech
International
Corporation

ManTech Security Technologies Corporation

- 1982 - 2002 Information Assurance and Counterintelligence
- 535 Staff
- Specialization in Risk Management
 - **Threat, vulnerability, and risk assessment (OMB A-130)**
 - **Cost-effective solutions (OMB A-94)**

Page 3



Secure Systems
and Infrastructure
Solutions



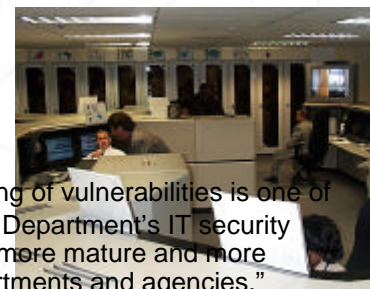
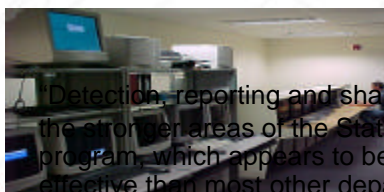
Information
Technology
Solutions



Systems
Engineering
Solutions

ManTech
International
Corporation

Worldwide Network Monitoring




"Detection, reporting and sharing of vulnerabilities is one of the stronger areas of the State Department's IT security program, which appears to be more mature and more effective than most other departments and agencies."


OMB GISRA Report to Congress

Page 4






Secure Systems and Infrastructure Solutions



Information Technology Solutions




Systems Engineering Solutions


ManTech
International Corporation

SBU System Monitoring

- Complete Design, Engineering, and Life Cycle Support
- 250+ Locations Worldwide
- 95+ Domestic Locations
- Integrated Threat Analysis and Incident Response Programs



Page 5





ManTech Security Technologies Corporation

Baseline Tool Kit - Security Configuration System



Secure Systems and Infrastructure Solutions




Information Technology Solutions




Systems Engineering Solutions

The Convergence of National Security and Technology






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions




Systems
Engineering
Solutions


ManTech
International
Corporation

Evolution of Cyber Security


- Complexity of cyber security has increased exponentially in distributed systems compared to main frame environments
- System management and configuration problems have resulted in chronic security vulnerabilities in most enterprise systems
- FISMA assigns responsibility to the CIO for the management systems and the security configuration required to reduce risk to an acceptable level (IAW OMB A-130)
- “Assurance” refers to activities to ensure that risk is in fact adequately mitigated

Page 7






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions




Systems
Engineering
Solutions


ManTech
International
Corporation

E-Gov Act and FISMA


- E-Government Act (Public Law 107-347) signed by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States.
- Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Page 8






Secure Systems and Infrastructure Solutions



Information Technology Solutions

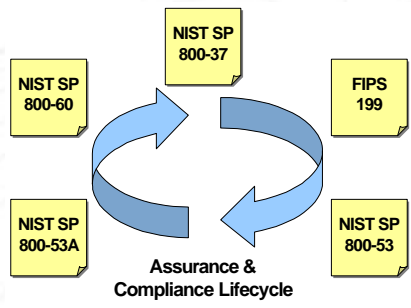


Systems Engineering Solutions

ManTech
International Corporation


NIST Assurance Vision


- Identify and categorize information and systems
- Prioritize the criticality of these resources
- Develop, implement and test strong security controls
- Establish minimum security control requirements
- *Establish a continuing program for monitoring security controls and configuration management, and reuse this data to support other aspects of a comprehensive security program (i.e., situational awareness capability)*




Assurance & Compliance Lifecycle

Page 9






Secure Systems and Infrastructure Solutions



Information Technology Solutions




Systems Engineering Solutions


ManTech
International Corporation

NIST Special Publications


- **NIST Special Publication 800-18**
Guide for Developing Security Plans for Information Technology Systems,
- **NIST Special Publication 800-30**
Risk Management Guide for Information Technology Systems,
- **NIST Special Publication 800-37**
Guide for the Security Certification and Accreditation of Federal Information Systems,
- **NIST Special Publication 800-53**
Guide for the Selection and Specification of Security Controls for Federal Information Systems
- **NIST Special Publication 800-53A**
Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems
- **NIST Special Publication 800-60**
Guide for Mapping Types of Information and Information Systems to Security Objectives and Risk Levels
- **FIPS Publication 199**
Standards for Security Categorization of Federal Information and Information Systems

Page 10





Secure Systems and Infrastructure Solutions



Information Technology Solutions




Systems Engineering Solutions


ManTech
International Corporation

Business Case – Checklist Development


- Internet Access Identified As Priority For Department
- Configuration Issues Identified One Source Of Vulnerabilities
- Sandia Penetration Test Revealed Significant Risk Associated With Vulnerabilities
- IATO And Connection Approval Sought On Basis Of IV&V
- Risk Management Approach Approved Based On Successful Completion of IV&V

Page 11






Secure Systems and Infrastructure Solutions



Information Technology Solutions




Systems Engineering Solutions


ManTech
International Corporation

IV&V Assessments


- Used Established Configuration Guidelines Approved By NSA, enhanced by Client
- Issues with IV&V By Fielded Tiger Teams (350+ locations)
- Ineffective, Costly, And Tedious. Physical and Cyber Assessments were manual and did not encompass the entire environment.
- No Adequate Remote Monitoring Tools. Most were too costly, lacked functionality, or both

Page 12






Secure Systems and Infrastructure Solutions



Information Technology Solutions

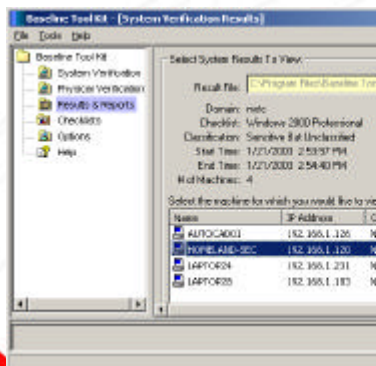



Systems Engineering Solutions

ManTech
International
Corporation

Baseline Tool Kit Overview

The Baseline Tool Kit is a Verification System developed to ensure Security Configuration Compliance for IA. The System consists of a lightweight Client application running on a Windows based computer as well as a relational database backend for storage of the data. Web Services are used for transmission and presentation of data. **Entire system developed 100% by cleared individuals.**



Secure Systems and Infrastructure Solutions



Information Technology Solutions




Systems Engineering Solutions

ManTech
International
Corporation


Baseline Tool Kit – Cyber Security

The Baseline Tool Kit has the ability to access security related data from all Windows based Computers running in a Domain, normalize the data into XML, and analyze the data against a configuration checklist to immediately identify mis-configurations on a Computer, Domain, or Entire system based on policy defined in the checklists.






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions

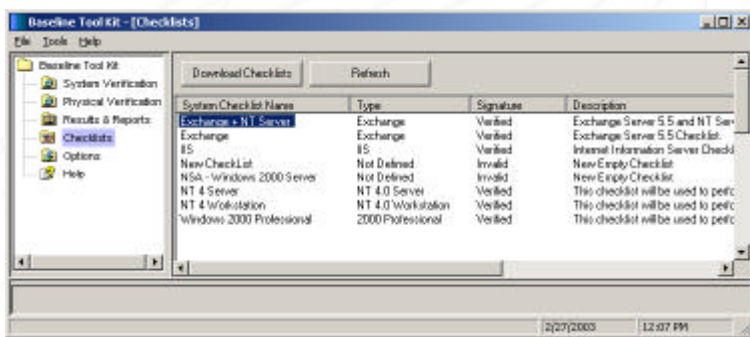


Systems
Engineering
Solutions


ManTech
International
Corporation


Centralized Configurations

- New and updated configuration checklists are downloaded from a central authority using Web Services, the latest industry technology standards for data exchange. Checklists may be configured using Configuration Standards from the NSA, Department of State, or your own internal Security policies.




Page 15






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions

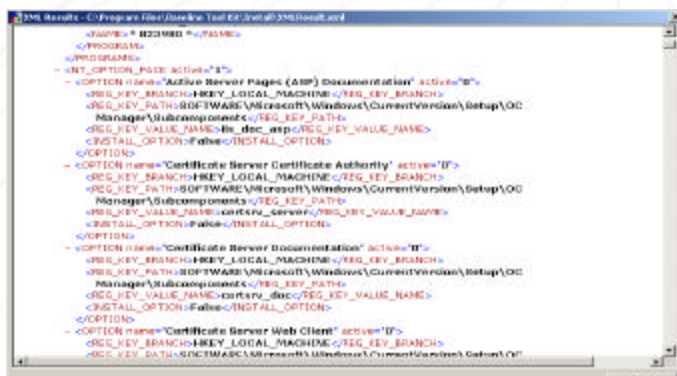


Systems
Engineering
Solutions

ManTech
International
Corporation

XML Checklists and Results

- All Checklists and Results are normalized into XML for standardization and easy of use. In-House Document Object Model (DOM) created for checklists and Results.
- All Items assigned unique number defining the check
- All items assigned a weight based on the Analysis Risk Model (ARM)





Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions



Systems
Engineering
Solutions

ManTech
International
Corporation

Computer Checklists Capabilities

Each Individual checklist item is assigned a unique **number** and **weight** to assign the Risk. The following sections of a computer are scanned by the Baseline Tool Kit

- **Account Policies**
- **Anti-Virus** (Service, Definition File age)
- **Audit Policies**
- **Control Panel** Settings (Screen Saver, Cached Profiles)
- **Disk Administrator** (NTFS, Dual Boot, Partitions)
- **Event Viewer** Settings
- **Exchange 2000** configurations
- **Files Permissions** (Exist, Not Exist, Advanced ACL's, File Version)
- **IIS Metabase** properties for All **Web** Sites and **FTP** Sites
- **Local Group** Membership
- **Local/Domain Users** (based on Account policies)
- **Network Protocols** (NetBIU, IPX)
- **Registry Settings** (Exists, Not Exists, Value, Advanced Permissions (10 levels)
- **Services** (Status, Type, Exists, Not Exists)
- **Installed Software** (32 bit Applications, Patches, Installed Components, Exists, Not Exists)
- **User Rights Policies**

Page 17



Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions



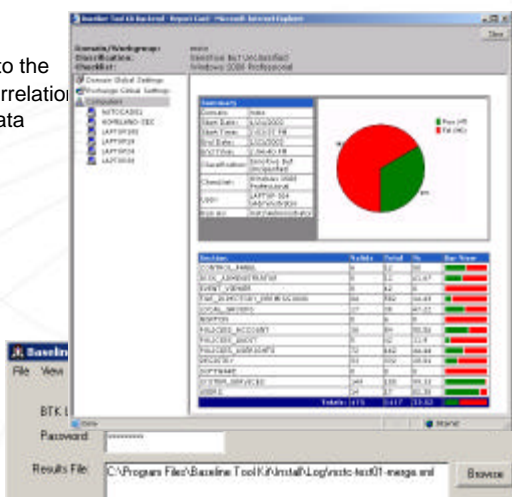
Systems
Engineering
Solutions

ManTech
International
Corporation

Centralized Results and Reporting

Results Data are Uploaded to the Backend for analysis and correlation with other security related data providing;

- Trend Analysis
- Customized Reporting
- Alerts
- Security Compliance
- Threat Modeling
- Life-Cycle Security
- Asset Management



Secure Systems and Infrastructure Solutions

Information Technology Solutions

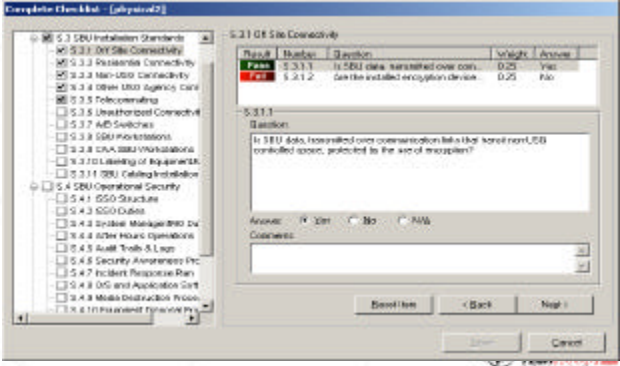
Systems Engineering Solutions

ManTech International Corporation

Physical Security

- Physical (Facilities) Security Checklists are integrated into the Baseline Tool Kit. Checklists are downloaded and uploaded through same process.
- Provides ability for automated integration of Physical and Cyber Security data for the entire Facility.

- Facilities Management
- Trend Analysis
- Complete Reporting
- Asset Management



Secure Systems and Infrastructure Solutions

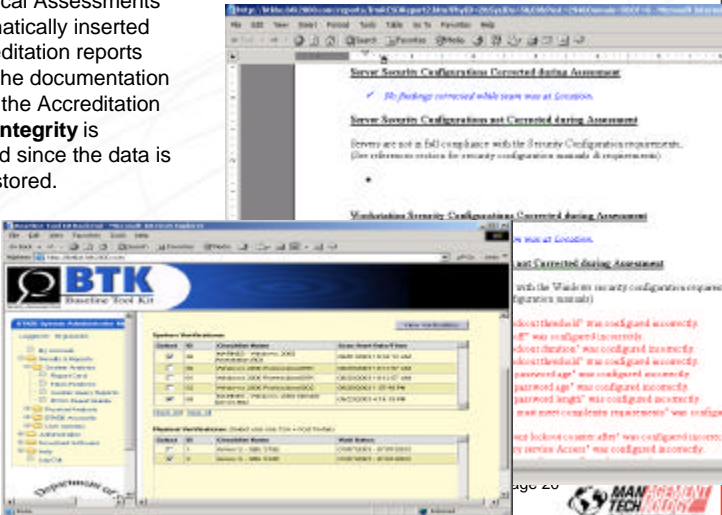
Information Technology Solutions


Systems Engineering Solutions

ManTech International Corporation


Automated Report Generation

Information from Computer and Physical Assessments are automatically inserted into Accreditation reports reducing the documentation phase for the Accreditation process. **Integrity** is maintained since the data is centrally stored.






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions




Systems
Engineering
Solutions


ManTech
International
Corporation

Baseline Tool Kit - Confidentiality


- Communication between client and Backend via Web Services using 128 Bit Secure Sockets Layer (SSL)
- One User ID / Password for both Systems.
- Microsoft Cryptographic Service Provider (CSP) utilized for **encryption** and **hashing** (MD5) (FIPS-140-1)
- Seven Different Access Levels for Data exposed from the Web Site.
- Three versions of the client based on installation key downloaded via Web Services.
 - Basic (No editing or viewing configuration checklists)
 - Advanced (No editing, able to view configuration checklists)
 - Administrator View, edit configuration checklists)
- All checklists are encrypted XML
- Backend Site secured in 12 FAM 600 compliant Network Operations Center
- Entire system Accredited via same C&A process used for all other systems.

Page 21






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions




Systems
Engineering
Solutions


ManTech
International
Corporation

Note on FIPS-140-1 and Microsoft


- While NIST Cryptographic Module Validation (CMV) accepts validation test reports for cryptographic modules against only FIPS 140-2 as of May 26, 2002, it states that agencies may continue to purchase, retain and use FIPS 140-1 validated products after May 25, 2002.
- Microsoft intends to submit cryptographic modules shipping with Windows Server 2003 for validation testing against FIPS 140-2.
- MS also intends to maintain the FIPS 140-1 validation status of cryptographic modules already shipped with Windows 2000 and Windows XP via their service packs.
- Four Microsoft cryptographic software components have completed the US Government FIPS 140-1 evaluation process;
 - The two **Microsoft default cryptographic services providers (CSPs)**
 - The Windows Kernel Mode Cryptographic Module
 - The Exchange Cryptographic Services provider (CSP)
- The Baseline Tool Kit (BTK) utilizes the default CSP for encrypting and hashing data.

Page 22






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions




Systems
Engineering
Solutions


ManTech
International
Corporation

Baseline Tool Kit - Integrity


- Configuration Checklists stored centrally as Binary objects in relational database.
- Checklists controlled by versioning
- Special Access level for ability to upload and maintain checklists.
- All BTK clients receive checklists via Web Services download. Download process hashes checklists creating a digital signature validating the checklist.
- All verification results are hashed creating a digital signature which prohibits tampering and ensures integrity of results.
- All results are marked with Classification level.
- Results cannot be uploaded unless the following criteria are met;
 - Checklist digital signature (hash) is valid.
 - Results digital signature (hash) is valid.
 - Classification level meets backend storage system classification.

Page 23






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions




Systems
Engineering
Solutions


ManTech
International
Corporation

Baseline Tool Kit - Authenticity


- Single ID/Password for entire System
- All Users Manually Validated before being Approved in System.
- Uploads/Downloads require Authentication
- Results XML Header contains;
 - ID used in the scan
 - Logged in User
 - Checklist that was used
- Results cannot be uploaded unless the following criteria are met;
 - Checklist digital signature (hash) is valid.
 - Results digital signature (hash) is valid.
 - Classification level meets backend storage system classification.

Page 24






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions




Systems
Engineering
Solutions


ManTech
International
Corporation

Baseline Tool Kit - Availability


- 1.5 Terabyte Storage Area Network
 - Redundant Fiber Arbitrated Loop direct to drive array
- Dual Dell 6650 SQL 2000 Servers
 - Microsoft Cluster Server (MSCS)
 - Two Node Active/Passive Configuration
- Dual 2650 Dell IIS 5.0 Servers
 - Network Load Balancing Service (NLBS)
 - Simple Object Access Protocol (SOAP)
 - Hosts Web Site and Accepts Web Services Requests
- 7x24 Network Operations Center (NOC)
 - 12 FAM 600 Guidelines

Page 25






Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions




Systems
Engineering
Solutions

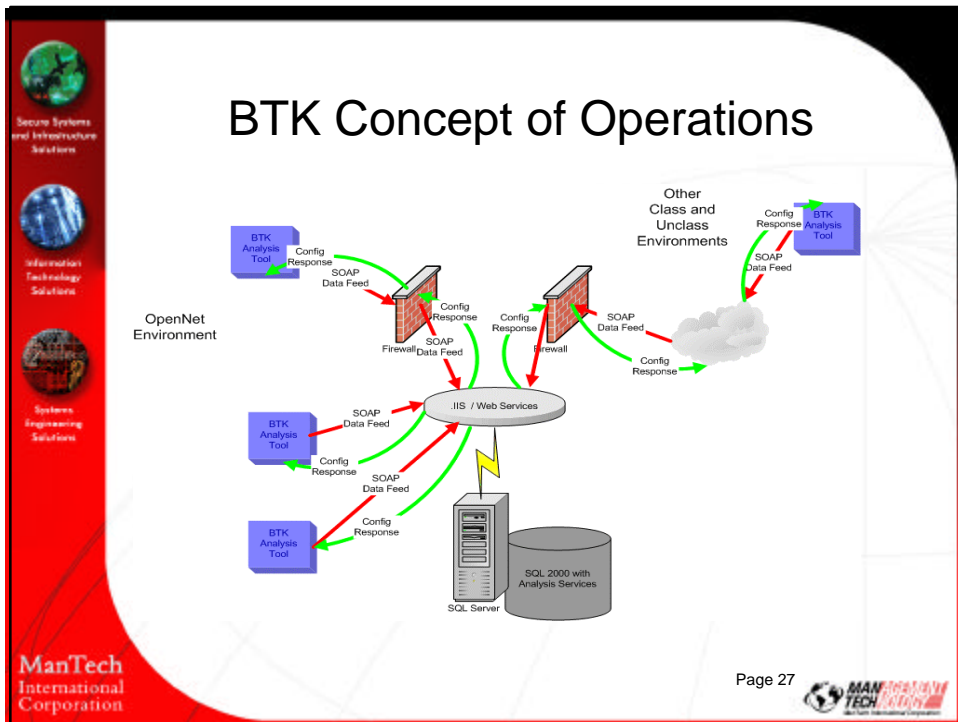
ManTech
International
Corporation

Baseline Tool Kit - Metrics

- 7 seconds per workstation (10 meg connection)
- 10 seconds per server (10 meg connection)
- 17 minutes/machine (192 k)
- Successful on lowest speed connection (64k)
- 600 machines in 8 hours
- 10 verifications simultaneously
- 360+ Locations worldwide targeted for Remote Assessment.
- 100% of machines analyzed instead of 10-15% random selection

Page 26







Secure Systems
and Infrastructure
Solutions



Information
Technology
Solutions



Systems
Engineering
Solutions

ManTech
International
Corporation

Integration Of BTK With IDS

- World Class Capability To Correlate IDS Events and Specific Event Log entries With Security Configuration Data In Near Real Time
- Forensic Ability To Detect Changes In Configuration
- Integration and automation with Computer Incident Response System (CIRT) via Web Services
- Analysis, Correlation, and Data Mining of Multiple Data Sources via Three Dimensional Cubes.
- On-Demand and scheduled compliance checks using a centralized BTK Service to schedule and complete the scans.
- BTK Service will perform Patch Management verifications and automatically report back findings. Similar to IAVA process.
- Geographic representation of security compliance for entire environment.
- Integration of Router configurations

Page 29



Secure Systems
and Infrastructure
Solutions



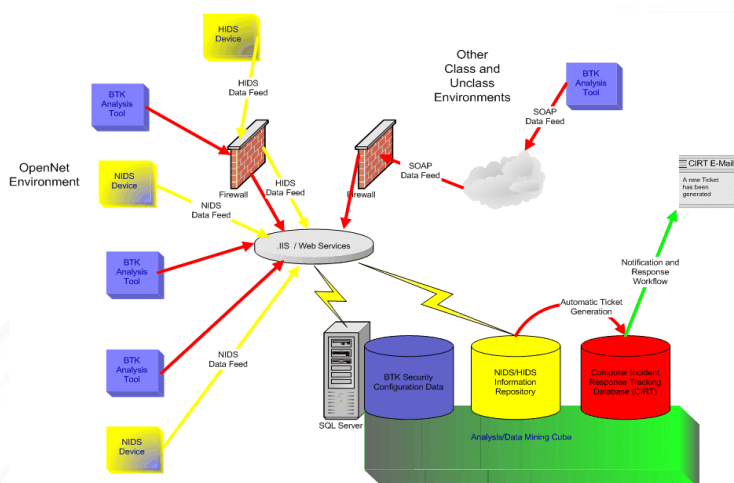
Information
Technology
Solutions



Systems
Engineering
Solutions

ManTech
International
Corporation

BTK / IDS Integration



Page 30



ManTech
Security Technologies Corporation
A ManTech International Company

Discussion



Secure Systems and Infrastructure Solutions Information Technology Solutions Systems Engineering Solutions

Q&A / Next Steps

The Convergence of National Security and Technology



Secure Systems and Infrastructure Solutions
Information Technology Solutions
Systems Engineering Solutions

ManTech Security Technologies Corporation
6400 Goldsboro Road
Suite 200
Bethesda, MD 20817
301-320-8917

ManTech International Corporation

Page 32

